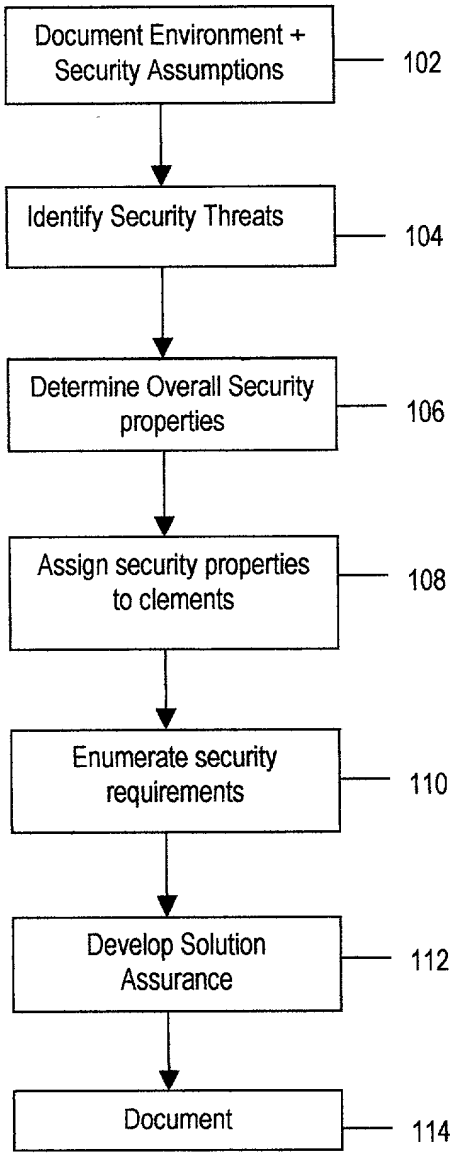
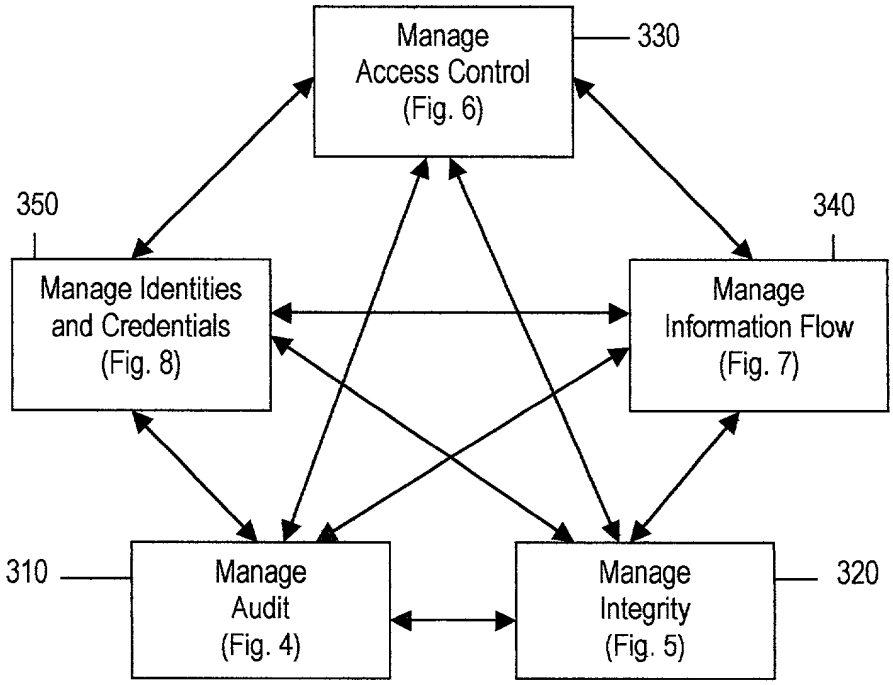

Document Environment + Security Assumptions
102
Identify Security Threats
104
Determine Overall Security properties
106
Assign security properties to clements
108
Enumerate security requirements
110
Develop Solution Assurance
112
Document
114

Fig. 1

Users, or processes
210
Acting in
Authorized
roles
212
Acquire, present and use
214
Credentials which convey
Identify and permissions
216
In order to
Request and receive
218
Authorization to
Invoke, or communicate with
220
Processes which
Access operate upon transfer distribute
222
Processes which
Normal Process Flow
Users, processes or others
210a
Acting in
Authorized or unauthorized
Roles, (either)
222
Acquire, present and use
214
Credentials which convey
Identity and permissions
216
In order to
Request and receive (or) circumvent
218a
Authorization to
Invoke, or communicate with, or observe flows related to
220a
Processes which
Access operate upon transfer destribute
222
Processes which
Peril Process Flow

Fig. 2



IT Security processes and subsystems

Fig. 3

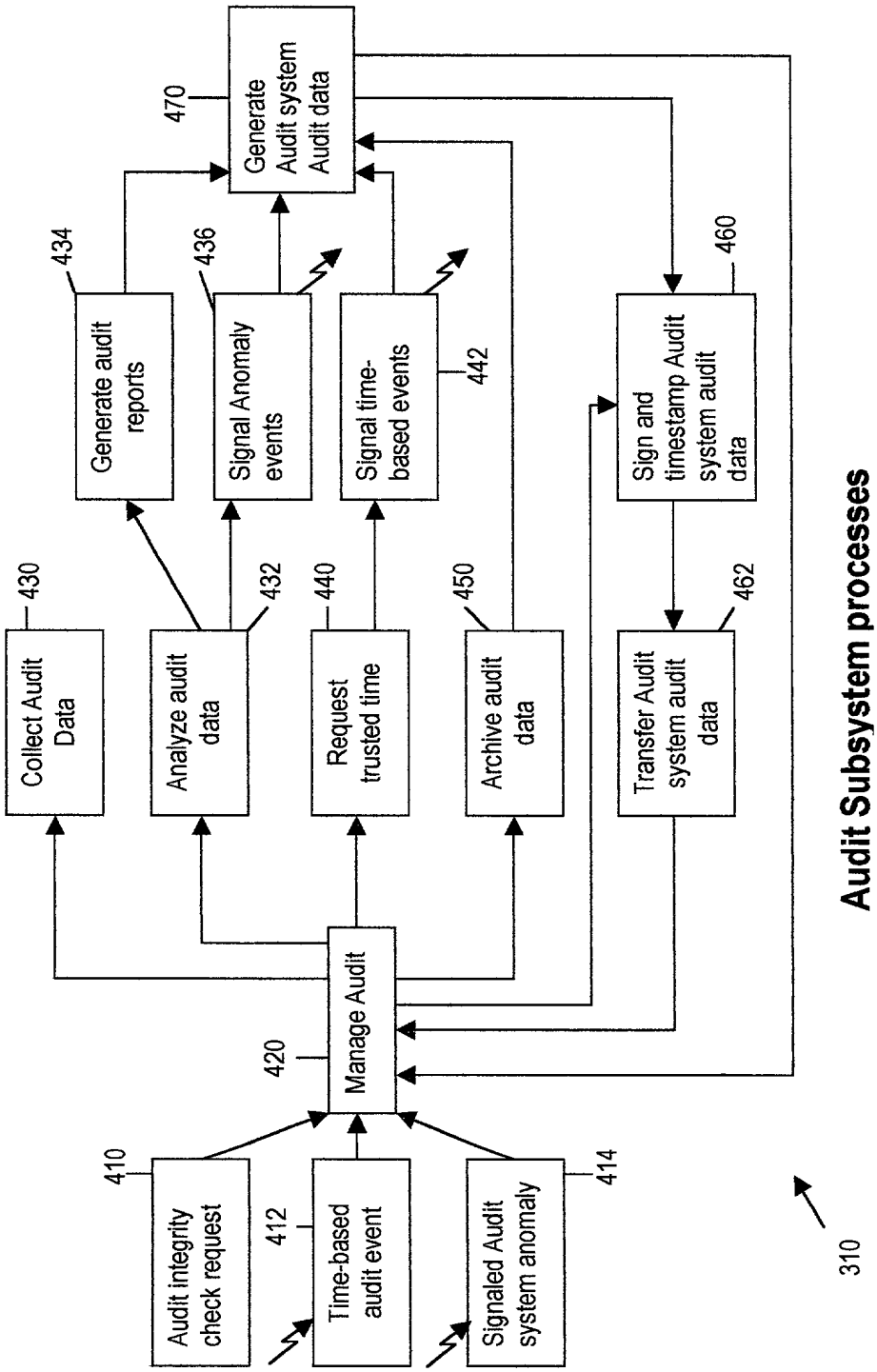
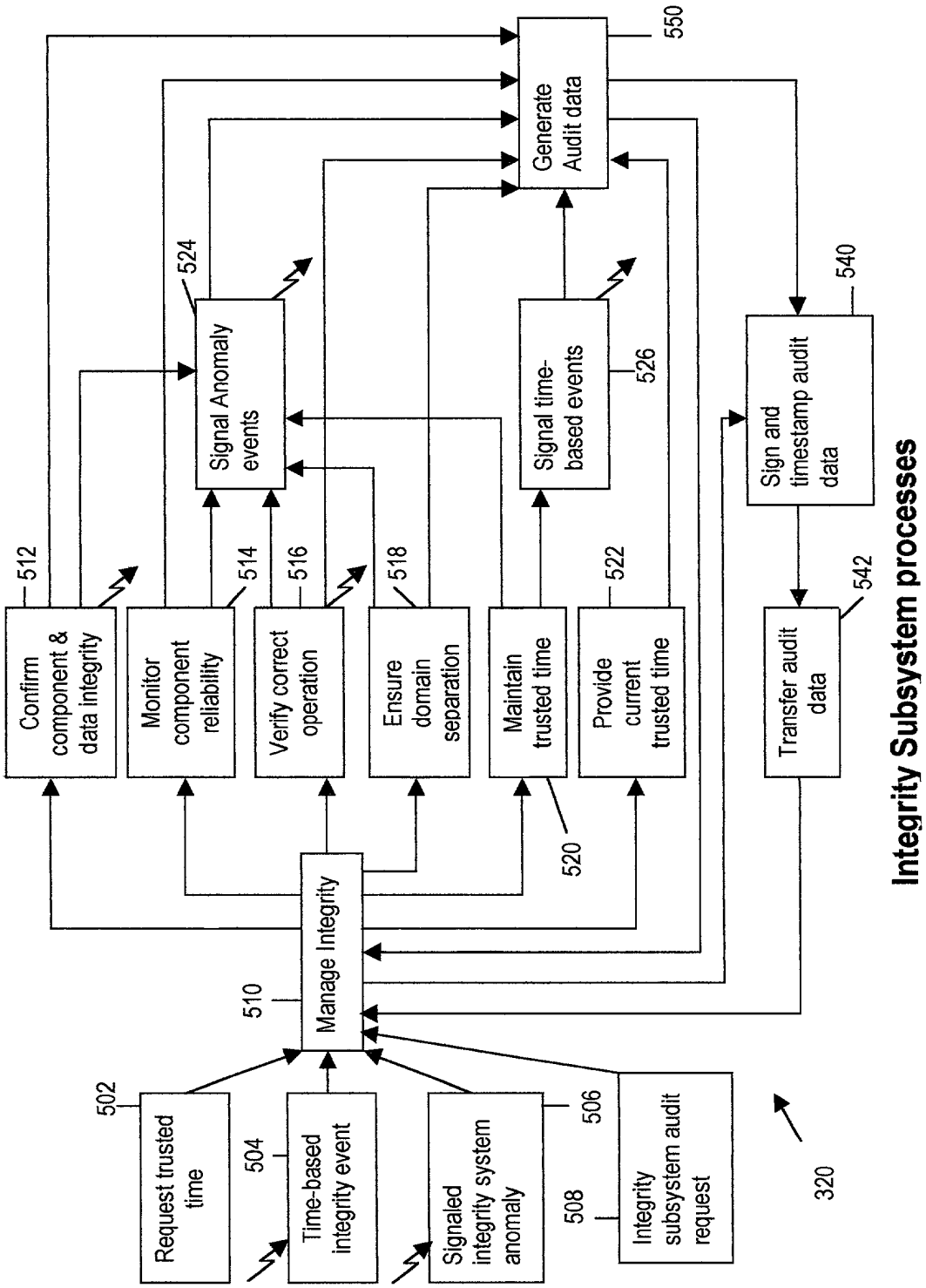

Audit Subsystem processes
310
Audit integrity check request
410
Time-based audit event
412
Signaled Audit system anomaly
414
Manage Audit
420
Collect Audit Data
430
Analyze audit data
432
Request trusted time
440
Archive audit data
450
Transfer Audit system audit data
462
Generate audit reports
434
Signal Anomaly events
436
Signal time-based events
442
Sign and timestamp Audit system audit data
460
Generate Audit system Audit data
470

Fig. 4



Integrity Subsystem processes

Fig. 5

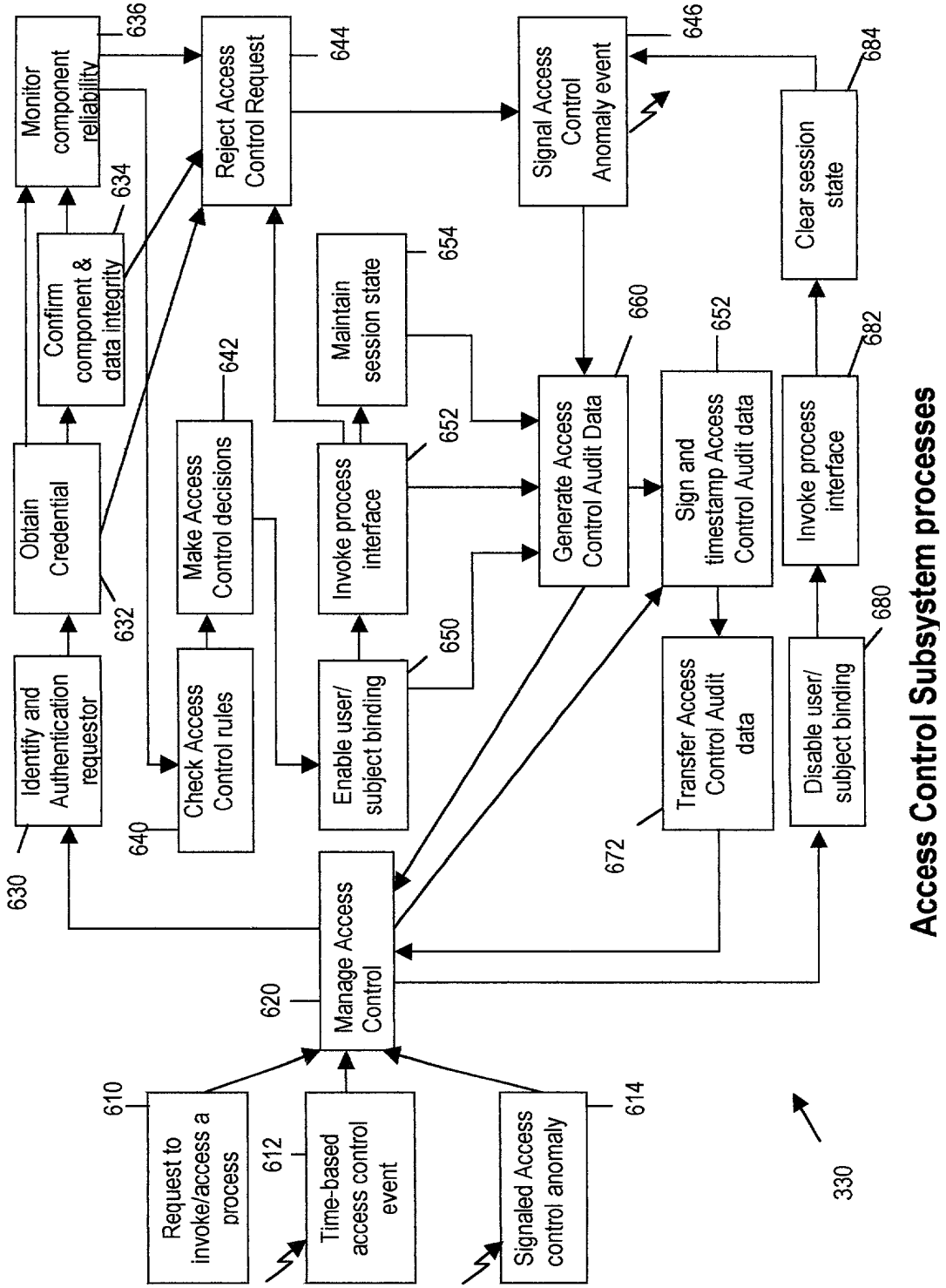
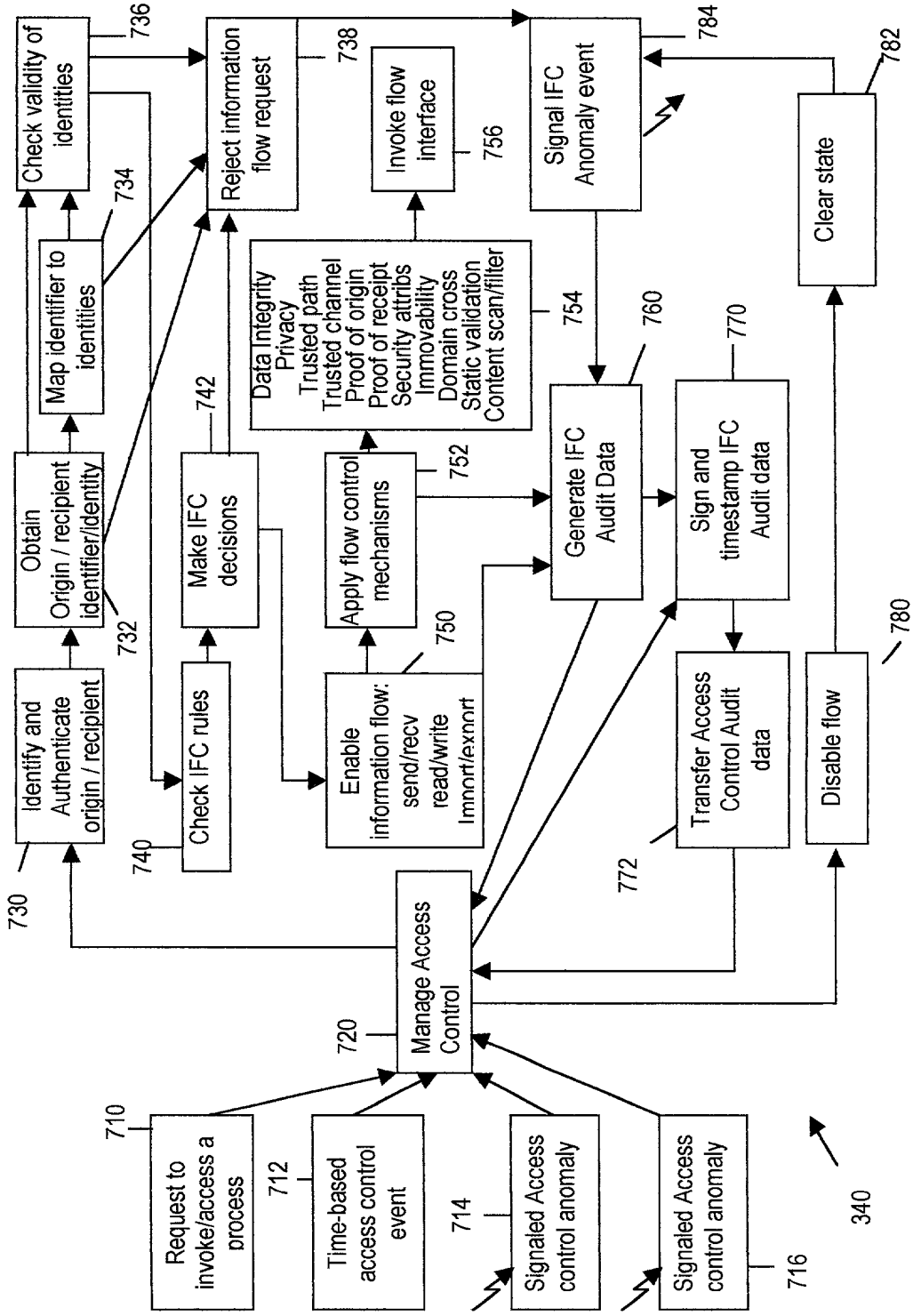


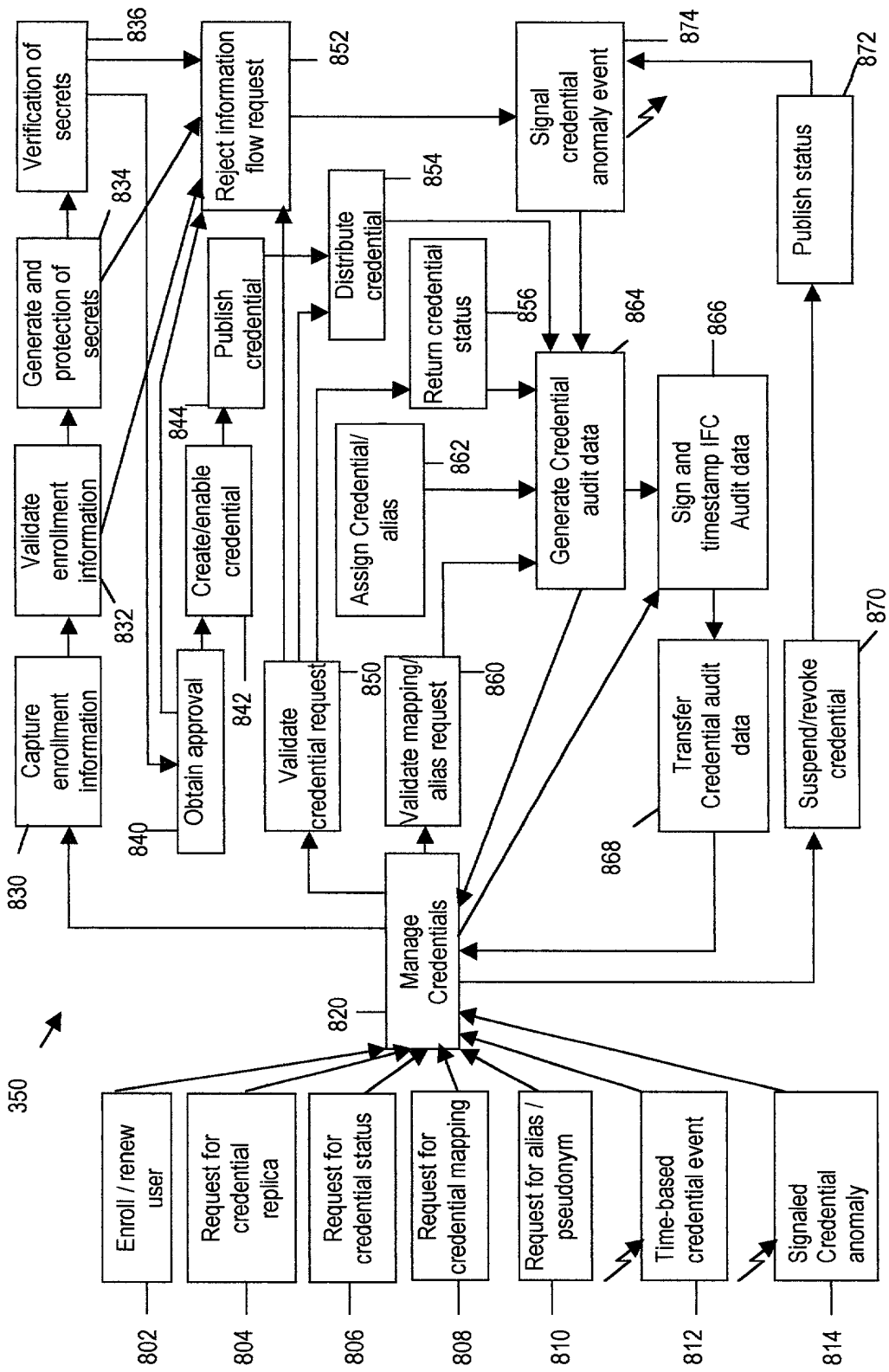
Fig. 6

Access Control Subsystem processes



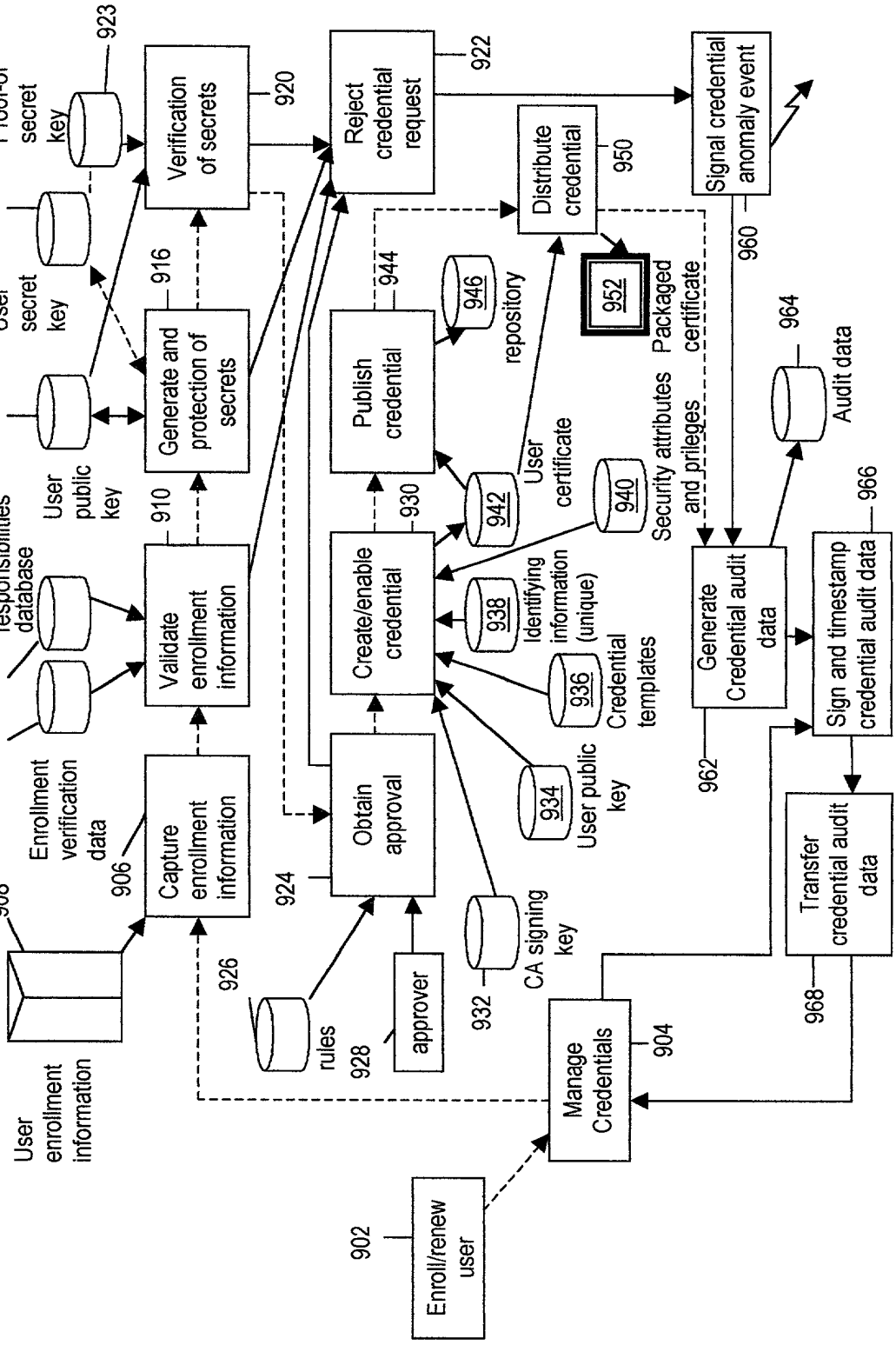
Information Flow Control Subsystem processes

Fig. 7



Credential Subsystem processes

Fig. 8



Sample PKI Digital Certificate Enrollment Process Flow

Fig. 9

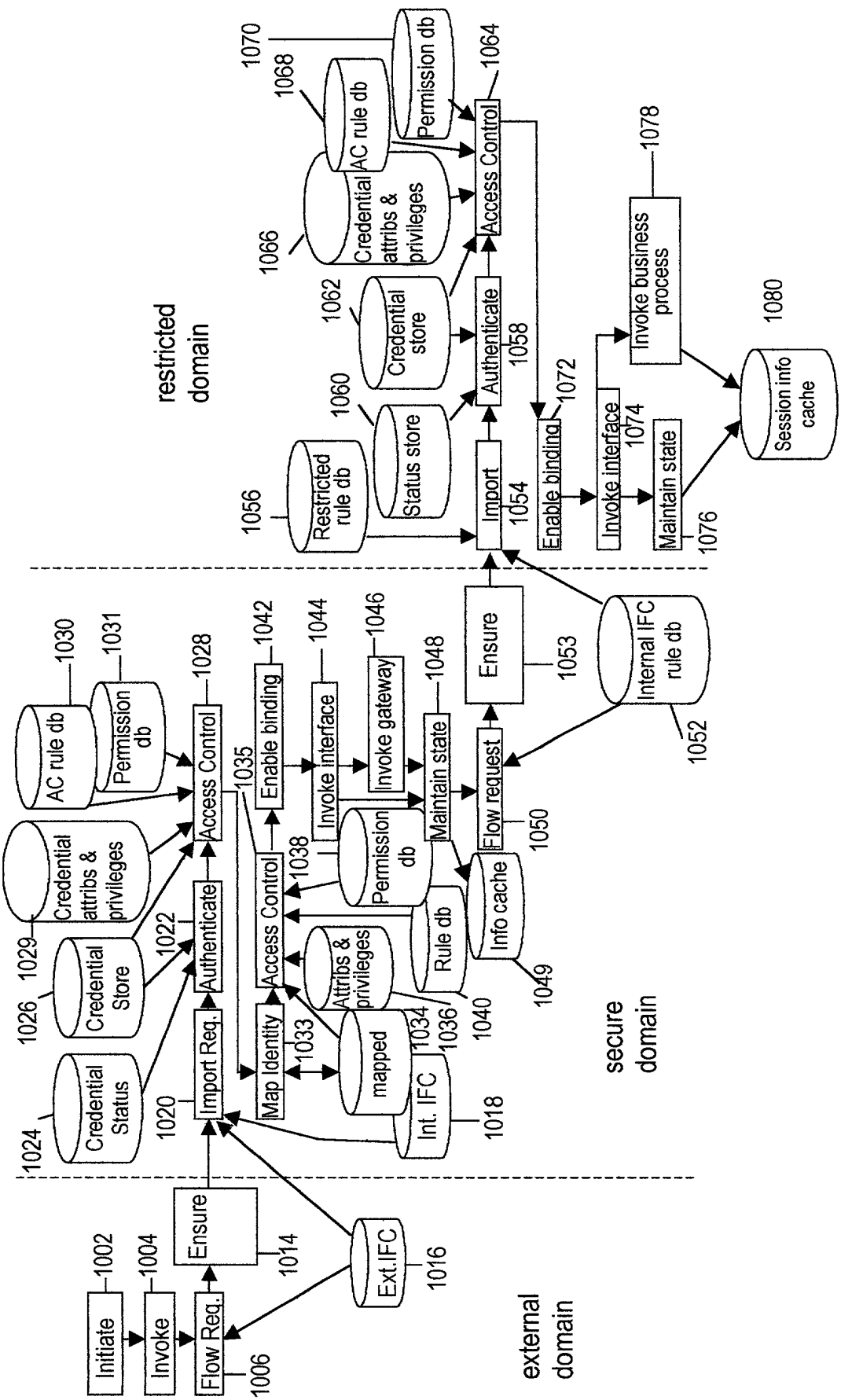

restricted domain
secure domain
external domain
Initiate
Invoke
Flow Req.
Ensure
Ext.IFC
Credential Status
Import Req.
Authenticate
Credential Store
Credential attribs & privileges
Access Control
AC rule db
Permission db
Map Identity
Access Control
Enable binding
Invoke interface
Invoke gateway
Attribs & privileges
mapped
Int. IFC
Permission db
Rule db
Maintain state
Info cache
Flow request
Ensure
Internal IFC rule db
Restricted rule db
Status store
Import
Authenticate
Credential store
Credential attribs & privileges
AC rule db
Permission db
Access Control
Enable binding
Invoke interface
Maintain state
Invoke business process
Session info cache
1002
1004
1006
1014
1016
1018
1020
1022
1024
1026
1028
1029
1030
1031
1033
1034
1035
1036
1038
1040
1042
1044
1046
1048
1049
1050
1052
1053
1054
1056
1058
1060
1062
1064
1066
1068
1070
1072
1074
1076
1078
1080

Fig. 10